FIRMWARE ANALYSIS AND COMPARISON TOOL

Firmware Analysis of NetBotz (APC - Schneider Electric) Rack Monitor 570/550/450 and Wall Monitor 455/355 - 4.5.3

Meta Data

HID	NetBotz (APC - Schneider Electric) Rack Monitor 570/550/450 and Wall Monitor 455/355 - 4.5.3
Device Name	Rack Monitor 570/550/450 and Wall Monitor 455/355
Vendor	NetBotz (APC - Schneider Electric)
Device Class	DVR
Version	4.5.3
Release Date	2016-11-02
Size	21.58 MiB (22,632,490 bytes)

Analysis

base64decoder

Time of Analysis	2018-03-29 13:02:26
Plugin Version	0.1.2

binwalk

Time of Analysis	2018-03-29 13:05:30
Plugin Version	0.5
Signature Analysis:	

DECIMAL HEXADECIMAL DESCRIPTION
——

0 0x0 uImage header, header size: 64 bytes, header CRC: 0x759DDD, created: 2016-09-30 15:50:56, image size: 22632426 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0x3E9EC215, OS: Linux, CPU: PowerPC, image type: RAMDisk Image, compression type: gzip, image name: "V4_5_3_20160930_1058"

64 0x40 gzip compressed data, maximum compression, has original file name: "nbroot.img", from Unix, last modified: 2016-09-30 15:50:46

303531 0x4A1AB Zlib compressed data, best compression
629636 0x99B84 Zlib compressed data, best compression
1022587 0xF9A7B Zlib compressed data, best compression
1059878 0x102C26 Zlib compressed data, best compression
1973137 0x1E1B91 Zlib compressed data, best compression
2107913 0x202A09 Zlib compressed data, best compression
2242911 0x22395F Zlib compressed data, best compression
2400190 0x249FBE Zlib compressed data, best compression
2533408 0x26A820 Zlib compressed data, best compression
2666213 0x28AEE5 Zlib compressed data, best compression
2732110 0x29B04E Zlib compressed data, best compression
2866178 0x2BBC02 Zlib compressed data, best compression
2999697 0x2DC591 Zlib compressed data, best compression
3015598 0x2E03AE Zlib compressed data, best compression
3069684 0x2ED6F4 Zlib compressed data, best compression
3134812 0x2FD55C Zlib compressed data, best compression
3254426 0x31A89A Zlib compressed data, best compression
3389796 0x33B964 Zlib compressed data, best compression
3588671 0x36C23F Zlib compressed data, best compression
3937563 0x3C151B Zlib compressed data, best compression
4049718 0x3DCB36 Zlib compressed data, best compression
4137491 0x3F2213 Zlib compressed data, best compression
4429049 0x4394F9 Zlib compressed data, best compression
4562407 0x459DE7 Zlib compressed data, best compression
4697515 0x47ADAB Zlib compressed data, best compression
4762444 0x48AB4C Zlib compressed data, best compression
4778360 0x48E978 Zlib compressed data, best compression
4897363 0x4ABA53 Zlib compressed data, best compression
4966890 0x4BC9EA Zlib compressed data, best compression
5031731 0x4CC733 Zlib compressed data, best compression
5166675 0x4ED653 Zlib compressed data, best compression
5420647 0x52B667 Zlib compressed data, best compression
5436766 0x52F55E Zlib compressed data, best compression
5617066 0x55B5AA Zlib compressed data, best compression
5750498 0x57BEE2 Zlib compressed data, best compression
5885114 0x59CCBA Zlib compressed data, best compression
6020374 0x5BDD16 Zlib compressed data, best compression
6248620 0x5F58AC Zlib compressed data, best compression
6264932 0x5F9864 Zlib compressed data, best compression
6321988 0x607744 Zlib compressed data, best compression
6505797 0x634545 Zlib compressed data, best compression
6706177 0x665401 Zlib compressed data, best compression
6839409 0x685C71 Zlib compressed data, best compression
6974943 0x6A6DDF Zlib compressed data, best compression
7132703 0x6CD61F Zlib compressed data, best compression
7267904 0x6EE640 Zlib compressed data, best compression
7332774 0x6FE3A6 Zlib compressed data, best compression
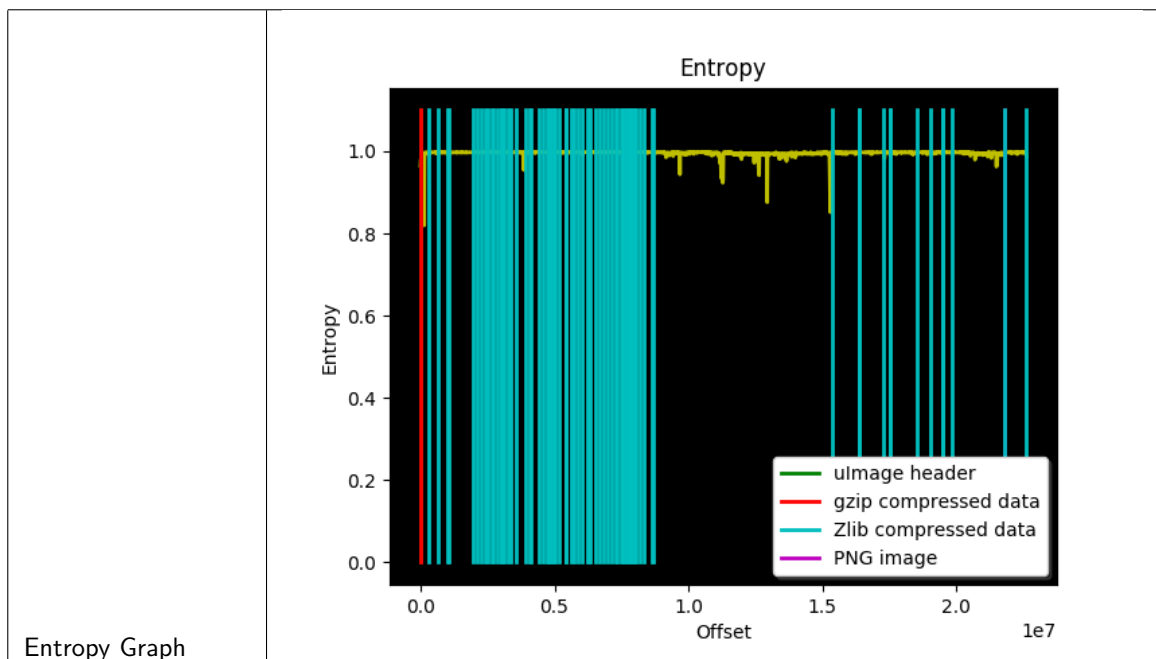7468473 0x71F5B9 Zlib compressed data, best compression
7537579 0x7303AB Zlib compressed data, best compression
7602625 0x7401C1 Zlib compressed data, best compression
7672286 0x7511DE Zlib compressed data, best compression
7737813 0x7611D5 Zlib compressed data, best compression

Entropy Graph

cpu architecture

Time of Analysis	2018-03-29 13:06:10
Plugin Version	0.3.1

crypto material

Time of Analysis	2018-03-29 13:02:05
Plugin Version	0.5

exploit mitigations

Time of Analysis	2018-03-29 13:06:14
Plugin Version	0.1.1

file hashes

Time of Analysis	2018-03-29 13:06:19
Plugin Version	1.0
imphash	None
md5	aff3ed2821d4a3c0e1cb0a56c0048393
ripemd160	450c7e078958fd4b58214005acb44a7fc36c6f58
sha1	164eb4233b78da456232c082dcaf5a0dd4021919
sha256	26ef025078abda69d2c3de06e27142a6db1a6385bd2524ce4976211570264a39
sha512	da38955f0df1be8e9713967c6d2e5d5d27ca1bd421e96f9159ab802b4586d 8b4b1fe62dbb2092ed4b8521986d25724e0a54e308ae993ddea899bb462386c3441
ssdeep	393216:JCWk8T1ykEFKvGf+/9vFmYS678jcZOzzyHGUPccDuHiWcCWTi0PlhH a:a8TokvQ+lU2tOzQPuCWyTXlh6
whirlpool	2517d24d06ac652e06bfbb32b4b1a70e899a6b0a48963e9f2262204a3e303 b80f6e44c66027781ed412557df4bf64bd3b78819017401ea50104d609df0ad1e02

file type

Time of Analysis	2018-03-29 13:05:56
Plugin Version	1.0
File Type	uImage header, header size: 64 bytes, header CRC: 0x759DDD, created: Fri Sep 30 15:50:56 2016, image size: 22632426 bytes, Data Address: 0x0, Entry Point: 0x0, data CRC: 0x3E9EC215, OS: Linux, CPU: PowerPC, image type: RAMDisk Image, compression type: gzip, image name: "V4_5_3_20160930_1058"
MIME	firmware/u-boot

init systems

Time of Analysis	2018-03-29 13:05:59
Plugin Version	0.4.1

ip and uri finder

Time of Analysis	2018-03-29 13:01:59
Plugin Version	0.4.1
IPs v4	list is empty
IPs v6	83::
	::9F
	::a
	::2D2
	2::7
	::
	7::
	C::
	5::

	1::
	::B
	F::
	::3
	::E
	8::
	3::b
	02::
	E2::
	c::
	6::E
	::F
	::c
	6::
	4::
	0::A
	::bF
	::4
	B::
	::e
	::8
	61::5
	::d
	E::
	::5
	9::D3
	a::
	A::
	D::
URIs	list is empty

software components

Time of Analysis	2018-03-29 13:05:50
Plugin Version	0.3

printable strings

Time of Analysis	2018-03-29 13:05:39
Plugin Version	0.2
string count	45253

users and passwords

Time of Analysis	2018-03-29 13:05:47
Plugin Version	0.4

string evaluator

Time of Analysis	2018-03-29 13:06:08
Plugin Version	0.2
string count	45253

unpacker

Time of Analysis	2018-03-29 13:01:18
Plugin Version	0.1
Plugin	Uboot
Extracted	2
size packed -> unpacked	21.57 MiB -> 21.58 MiB
entropy	0.89

malware scanner

Time of Analysis	2018-03-29 13:05:52
Plugin Version	0.3
MD5	aff3ed2821d4a3c0e1cb0a56c0048393
System Version	0.2.6
Scanners Number	1
Positives	0
Scanners	ClamAV
Scanns	ClamAV :: result:clean ClamAV :: detected:False ClamAV :: version:ClamAV 0.99.4/24430/Thu Mar 29 06:23:16 2018